Amendments to the Claims:

A listing of the entire set of pending claims (including amendments to the claims, if any) is submitted herewith per 37 CFR 1.121. This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently amended) A secure communication system including

a source device and

at least one sink device; information being transferred from the source device to the sink device in a communication session including the transfer of a plurality of packets from the source device to the sink device; each packet including a data field for transferring a portion of the information;

the source device including:

a key generator for, at the initiative of the source device, generating an active source session key in a predetermined sequence of source session keys $Ksource_i$;

an encryptor for encrypting at least part of the data field of a packet under control of the active source session key; the encrypted part of the data field including a sub-field designated as a key check block field;

the sink device including:

a key generator for generating a plurality of candidate sink session key in a predetermined sequence of sink session keys $Ksink_i$, where for each index i in the sequence the respective sink session key $Ksink_i$ corresponds to the respective source session key $Ksource_i$;

a decryptor for decrypting at least part of the data field of a received packet under control of a sink session key;

a key resolver operative

to determine which of the candidate sink session keys corresponds to the source session key used to encrypt the encrypted part of a received packet, by causing the decryptor to decrypt the data in the key check block field of the received packet under control

PAGE 2/9 * RCVD AT 4/11/2005 8:58:02 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID:2152437525 * DURATION (mm-ss):02-46

of ~~each time~~ a different one of the plurality of candidate sink session keys until a valid decryption result is found; and

to cause the decryptor to decrypt a remaining encrypted part of the data field of the packet under control of the candidate sink session key which produced the valid decryption result.

2. (Original) A secure communication system as claimed in claim 1, wherein

the plain-text form of the key check block in the key check block field is a public data block.

3. (Original) A secure communication system as claimed in claim 1, wherein

the plain-text form of the key check block in the key check block field is a data block agreed between the source and sink device before starting the transfer of the information and used for the entire communication session.

4. (Original) A secure communication system as claimed in claim 1, wherein

the plain-text form of the key check block in the key check block field changes at least once during the communication session.

5. (Original) A secure communication system as claimed in claim 4, wherein

the source and sink device include corresponding key check block generators for generating the plain-text form of the key check block and effecting the change of the plain-text form of the key check block.

6. (Original) A secure communication system as claimed in claim 4, wherein

the plain-text form of the key check block of a particular packet is derived from information transferred in a packet preceding the particular packet.

7. (Original) A secure communication system as claimed in claim 6, wherein

the plain-text form of the key check block is derived from information transferred in a packet immediately preceding the particular packet.

8. (Previously presented) A secure communication system as claimed in claim 6, wherein

the plain-text form of the key check block of a particular packet is identical to the plain-text form of a predetermined data block, other than the key check block, in an encrypted part of the data field of a packet preceding the particular packet.

9. (Currently amended) A sink device for use in a secure communication system wherein a source device autonomously can change a source session key used for encrypting at least part of the data field of a packet transferred from the source device to the sink device; the encrypted part of the data field including a sub-field designated as a key check block field; the sink device including:

a key generator for generating a plurality of candidate sink session key in a predetermined sequence of sink session keys $Ksink_i$, where for each index i in the sequence the respective sink session key $Ksink_i$ corresponds to the respective source session key $Ksource_i$;

a decryptor for decrypting at least part of the data field of a received packet under control of a sink session key;

a key resolver operative

to determine which of the candidate sink session keys corresponds to the source session key used to encrypt the encrypted part of a received packet, by causing the decryptor to decrypt the data in the key check block field of the received packet under control of ~~each time~~ a different one of the plurality of candidate sink session keys until a valid decryption result is found; and

to cause the decryptor to decrypt a remaining encrypted part of the data field of the packet under control of the candidate sink session key which produced the valid decryption result.

PAGE 4/9 * RCVD AT 4/11/2005 8:58:02 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID:2152437525 * DURATION (mm-ss):02-46

10. (Currently amended) A method of secure communication between a source device and at least one sink device; information being transferred from the source device to the sink device in a communication session including the transfer of a plurality of packets from the source device to the sink device; each packet including a data field for transferring a portion of the information; the method including:

at the initiative of the source device generating an active source session key in a predetermined sequence of source session keys $Ksource_i$;

encrypting at least part of the data field of a packet under control of the active source session key; the encrypted part of the data field including a sub-field designated as a key check block field;

transferring the packet from the source device to the sink device;

generating a plurality of candidate sink session key in a predetermined sequence of sink session keys $Ksink_i$, where for each index i in the sequence the respective sink session key $Ksink_i$ corresponds to the respective source session key $Ksource_i$;

determining which of the candidate sink session keys corresponds to the source session key used to encrypt the encrypted part of a received packet, by decrypting the data in the key check block field of the received packet under control of ~~each time~~ a different one of the plurality of candidate sink session keys until a valid decryption result is found; and

decrypting a remaining encrypted part of the data field of the packet under control of the candidate sink session key which produced the valid decryption result.

PAGE 5/9 * RCVD AT 4/11/2005 8:58:02 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID:2152437525 * DURATION (mm-ss):02-46

11. (Currently amended) A method of in a sink device in a secure communication system detecting a change of a session key effected by a source device in the system; information being transferred from the source device to the sink device in a communication session including the transfer of a plurality of packets from the source device to the sink device; each packet including a data field for transferring a portion of the information; at least part of the data field of a packet being encrypted under control of an active source session key in a predetermined sequence of source session keys $Ksource_i$; the encrypted part of the data field including a sub-field designated as a key check block field; the method including:

generating a plurality of candidate sink session key in a predetermined sequence of sink session keys $Ksink_i$, where for each index i in the sequence the respective sink session key $Ksink_i$ corresponds to the respective source session key $Ksource_i$;

determining which of the candidate sink session keys corresponds to the source session key used to encrypt the encrypted part of a received packet, by decrypting the data in the key check block field of the received packet under control of ~~each time~~ a different one of the plurality of candidate sink session keys until a valid decryption result is found; and

decrypting a remaining encrypted part of the data field of the packet under control of the candidate sink session key which produced the valid decryption result.

12. (Original) A computer program product where the program product is operative to cause a computer to perform the method of claim 11.

PAGE 6/9 * RCVD AT 4/11/2005 8:58:02 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID:2152437525 * DURATION (mm-ss):02-46